Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2004 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2004

Information Technology as a Target and Shield in Urban Environments

Laura Lally
Hofstra University

Information Technology as a Target and Shield in Urban Environments

Laura Lally
Hofstra University
acslhl@hofstra.edu

ABSTRACT

This paper presents Lally's Target and Shield model which addresses how Information Technology can be used as a target in terrorist and other malicious attacks. The model also addresses ways that Information Technology can be used as a shield to prevent further attacks and mitigate their impact if they should occur. The Target and Shield model is grounded in Normal Accident Theory and the Theory of High Reliability Organizations, both of which address the prevention of innocent errors propagating into major accidents in organizational settings. The paper will explore the challenges of extending this model to encompass deliberate malicious acts in large urban areas. Emerging IT based initiatives for combating terrorist attacks will be presented in the context of the model. Methodologies for further validating the model conclude the paper.

Keywords

Computer security, Computer privacy, Normal Accident Theory, Theory of High Reliability Organizations, Urban IT, Post 9/11, Terrorism, Target and Shield Model.

INTRODUCTION: POST 9/11 IT CHALLENGES TO URBAN ENVIRONMENTS

In the Post 9/11 environment, Information Technology **(IT)** Security has become a growing issue in large urban environments likely to be the target of such attacks because of their critical masses of people and complex, critical infrastructures. Yourdon (2002, p. 205) states:

> IT managers face more sophisticated and malevolent forms of attacks on these systems. Unlike the Y2K, problem, which was the result of an innocent bad judgement, "the disruptive shocks to our organizations are no longer accidental, benign, or acts of nature; now they are deliberate and malevolent".

Increased reliance on computer based systems adds to the vulnerability and to the potential for widespread effects, particularly in large urban areas. DETER and EMIST (2004, p. 58) argue:

> As the Internet has become pervasive and our critical infrastructures have become inextricably tied to information systems, the risk for economic, social and physical disruption due to the insecurities of information systems has increased immeasurably.

Furthermore, IT based systems may also be used as a weapon in attacks against other key infrastructure systems such as electric power and water (National Research Council, 2002, p. 136). Designing secure, resilient systems in the face of these new threats will be a major challenge for large urban areas.

As the terrorist attacks of 9/11/01 and the blackout of 8/14/03 indicated, large urban areas need improved methodologies for dealing with large-scale catastrophes. IT based systems can be used to mitigate the impacts of the damage of both terror attacks and non-malicious accidents with proper design, implementation and training. This analysis will argue, therefore, that IT based systems are not only a **target**, a source of vulnerability, but that they can also be a **shield**, a means of combating the threats and mitigating the damage malicious individuals are able to accomplish.

This research will present Lally's (2004) **"Target and Shield"** conceptual model of the sources, propagation and potential impacts of IT related threats, as well as the means by which IT can be used to identify, eliminate and mitigate the damages caused by other sources of threats. The conceptual model draws on two theoretical perspectives, an extended version of Perrow's Normal Accident Theory, and the Theory of High Reliability Organizations.

THEORETCAL FOUNDATIONS

Normal Accident Theory (Perrow, 1984) argues that characteristics of a system's design make it more or less prone to accidents. Perrow distinguishes between disastrous "accidents," which are system wide and seriously impact the system's overall functioning and "incidents," which involve single failures that can be contained within a limited area and which do not compromise the system's overall functioning. Perrow argues that no system can be designed to completely avoid incidents, but that inherent qualities of the system determine how far and how fast the damage will spread. Systems that are not designed to contain the negative impact of incidents will, therefore, *be subject to accidents in the course of their normal functioning.*

The first key characteristic of accident prone systems is their complexity. Normal Accident Theory argues that as systems become more complex, they become more accident prone. Complex systems are also characterized by non-linear interactions and interactions that are invisible to the naked eye. Operators see only the "tip of the iceberg". Normal Accident Theory distinguishes a second characteristic of systems that exacerbate potential problems brought about as a result of complexity -- tight coupling. Tight coupling means there is no slack time or buffering of resources between tasks, interactions happen immediately. Both complexity and tight coupling are often more efficient from a productivity standpoint. However, incidents tend to propagate faster and their impact becomes more severe because there is no lag time during which human intervention can occur .

Researchers in High Reliability Organizations have examined organizations in which complex, tightly coupled, technologically based systems appeared to be coping successfully with the potential for disaster. They emphasize the importance of good communication, shared mental models of systems, shared values of the importance of safety, continual organizational learning, and redundancy of key systems (Grabowski & Roberts, 1997; La Porte & Consolini, 1991; Klein, Bigley, and Roberts, 1995; Sagan, 1993; Turner, 1976; Weick & Roberts, 1993,).

Lally (1996) argued that Normal Accident Theory was a sound theoretical perspective for understanding the risks of Information Technology, because IT is complex, and tightly coupled and often poorly controlled.

She also argued (Lally, 1996, 1997) that IT based systems do not operate in isolation but in organizational settings where failures in IT can lead to more widespread secondary failures in organizations. The secondary failures are also a major issue when IT is being used to support the safe operation of large urban areas. Additionally, she argued (Lally, 2002) that the frequent rapid change in both IT based systems and the work processes they support can further exacerbate the potential for disaster.

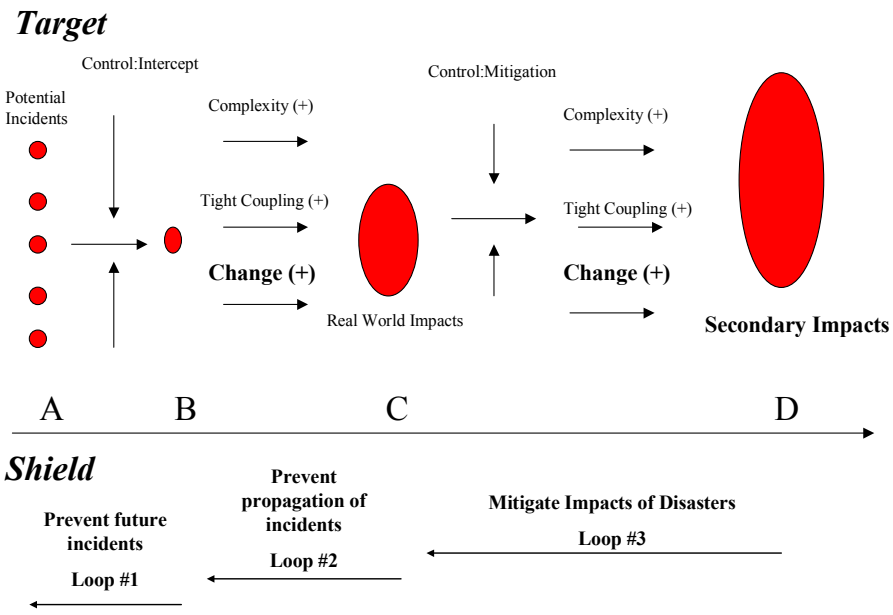
Lally (2004) further extended her model and argued that IT based systems are not only a **target** used as a weapon of destruction to cause serious accidents, but that IT based systems can be a **shield** used to prevent damage from future incidents, whether they be IT based or physical.

This **"Target and Shield"** conceptual model drew on insights from the Theory of High Reliability Organizations and suggests that IT designers and managers, as well as government and law enforcement agencies learn from past experiences and embody this knowledge in the design and implementation of future IT based systems. The resulting systems should not only be more secure and resilient, they should aid in preventing future IT based or physical attacks, or mitigating their impact should they occur.

Figure 1 illustrates the **Target and Shield** conceptual model for analyzing the source, propagation and impacts of IT based threats, as well as ways in which IT can be used to identify, and mitigate the impact of, future threats.

The Target and Shield model incorporates Lally's extensions to Normal Accident Theory. The model also contains *three significant feedback loops*, which allow IT to play a positive role in preventing future incidents from materializing, having real world impacts, and mitigating their impacts when they do occur. In the Feedback Loop #1, **Prevent future incidents**, controls can be built into the system to prevent future incidents from materializing. In Feedback Loop #2, **Prevent Propagation of Incidents**, controls can be built into the system to prevent future incidents that have materialized from turning into accidents. In the Feedback Loop #3, **Mitigate Impact of Disasters**, IT based systems can be developed to prevent accidents resulting from IT based or physical attacks from propagating even further.

Figure 1: The Target and Shield Model



The Target and Shield model, therefore, provides a framework for categorizing emerging Post 9/11 initiatives and understanding the role they will play in either: 1) eliminating sources of risk before they can do damage, 2) preventing small problems that do happen from becoming major problems, or 3) mitigating the damage of large scale disasters.

EXTENDING THE MODEL TO DELIBERATE ATTACKS IN LARGE URBAN AREAS

The Target and Shield model draws upon Normal Accident Theory and the Theory of High Reliability Organizations, theories used for the preventing innocent mistakes from propagating into system-wide disasters in organizational settings. Two key issues must be addressed when applying the model to 9/11 type attacks. First the model must be extended to address the possibility of deliberate attacks rather than innocent mistakes. Secondly, the model must be extended to address the challenges of applying the principles of these theories to large diverse urban environments, rather than organizational settings. Large urban areas add additional layers of complexity and tight coupling when compared to organizational settings. In organizational settings, the shared mental models recommended by High Reliability Theory are easier to enforce. Organizations can appoint professionals who are educated in preventing disasters and involve all employees in disaster training. Terrorist attacks in urban areas are likely to involve "a spectrum of trained professionals, cognitively and physically fatigued individuals, motivated volunteers, and frightened victims" (Murphy, 2004, p. 68), making shared mental models harder to achieve and appropriate social interaction harder to achieve. The complex, tightly coupled infrastructure of large urban areas makes fault isolation more difficult and system restoration more difficult to achieve, the blackout of 8/14/03 being the most striking recent example. IT based initiatives for combating terrorism must address these new challenges as well.

EVALUATING EMERGING INITIATIVES IN TERMS OF THE TARGET AND SHIELD MODEL

In terms of preventing future incidents (Feedback Loop #1) a number of IT based initiatives are emerging. They include:

> Language translation tools that can identify suspicious phrases in written communications (Popp, Armour, Senator, and Numrich, 2004).
>
> Pattern analysis tools that can help distinguish terrorist activities from activities that may appear similar but be non-malicious, such as legitimate building demolition (Popp, Armour, Senator, and Numrich, 2004).

Social network analysis that seeks to identify abnormal patterns of social interactions, such as terrorist "sleeper cells" becoming active (Coffman, Greenblatt, and Marcus, 2004).

Links to public safety related databases to help police identify potential terrorists and other criminals (Sawyer, Tapia, Pescheck, and Davenport, 2004).

All of these can help prevent terrorist attacks from taking place in urban areas.

In terms of preventing the propagation of future incidents (Feedback Loop #2) IT based initiatives include:

Improved forms of Cyber Defense beyond the traditional detect-respond paradigm (Saydjari, 2004).

An experimental infrastructure and rigorous scientific methodologies for developing and testing next generation cyber security technology (DETER and EMIST, 2004).

A Manhattan Project style approach to building a more secure infrastructure with the required large investments in technology and expertise (Saydjari, 2004).

These approaches should help designers of both technological and physical infrastructures create more secure and resilient systems in the future

In terms of mitigating the impact of future disasters (Feedback Loop #3), IT based initiatives are also emerging:

Software assistant agents that provide intelligence and communications links to first responders such as police and fireman responding to a suspicious fire. These systems enforce the concept of shared mental models recommended by High Reliability Theory (Kogut, Yen, Leung, Sun, Wang, Mielczarek, and Hellar, 2004).

Robots to help with rescue efforts in dangerous areas, such as Ground Zero following the 9/11 attacks (Murphy, 2004).

These systems can help first responders in large urban areas work together in a safer and more co-ordinated manner to mitigate the impacts of terrorist attacks.

CONTRIBUTIONS AND DIRECTIONS FOR FURTHER RESEARCH

The strength of the Target and Shield model is that it provides an original theory based framework for addressing key issues in IT security in urban areas. The model's weakness is that it requires further empirical validation. Emerging IT initiatives to counter terrorism in large urban areas map readily into the model. As these initiatives become realities, case studies of their implementation will provide new insight into the most appropriate design of new infrastructures as well as the most appropriate uses of IT to counter terrorism. When these innovations are used on a regular basis, more quantitative methodologies can address their efficiency and effectiveness.

This research was supported by a Summer Research Grant from the Frank G. Zarb School of Business at Hofstra University.

REFERENCES

1. Coffman, T., Greenblatt, S., and Marcus, S. (2004). Graph Based Technologies for Intelligence Analysis. Communications of the ACM, March, 45-47.

2. DETER and EMIST Projects. (2004). Cyber Defense Technology Networking and Evaluation. Communications of the ACM, March, 58-61.

3. Grabowski, M. and Roberts, K. (1997). Risk mitigation in large scale systems: Lessons from high reliability organizations. *California Management Review*, Summer, 152-162.

4. Klein, R.L., Bigley, G.A., Roberts, K.H. (1995). Organizational culture in High Reliability Organizations. *Human Relations*, 48:7. 771-792.

5. Kogut, P., Yen, J., Leung, Y, Sun, S. Wang, R., Mielczarek, T., and Hellar, B., (2004). Proactive Information Gathering for Homeland Security Teams, *Communications of the ACM,* March, 48-50.

6. Lally, L. (1996). Enumerating the risks of reengineered processes. *Proceedings of 1996 ACM Computer Science Conference***,** 18-23.

7. Lally, L. (1997). Are reengineered organizations disaster prone?" *Proceedings of the National Decision Sciences Conference,* 178-182.

8. Lally, L. (2002). Complexity, coupling, control and change: An IT based extension to Normal Accident Theory. *Proceedings of the International Information Resources Management Conference*, 1089-1095.

9. Lally, L. (2004) Information Technology as a Target and Shield in the Post 9/11 Environment. *Information Resources Management Journal,* upcoming.

10. LaPorte, T. R. & Consolini. P. (1991). Working in practice but not in theory: Theoretical challenges of High Reliability Organizations. *Journal of Public Administration,* 1, 19-47.

11. Murphy, R. (2004). Rescue Robotics for Homeland Security. Communications of the ACM, March, 66-68.

12. National Research Council. (2002). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism.* Washington, D.C.: National Academies Press.

13. Perrow, Charles. (1984) *Normal Accidents: Living with High Risk Technologies.* New York: Basic Books.

14. Popp, R., Armour, T., Senator, T., and Numrich, K. (2004) Countering Terrorism Through Information Technology. *Communications of the ACM*, March, 36-43.

15. Sagan, Scott. (1993). *The Limits of Safety*. Princeton New Jersey: Princeton University Press.

16. Sawyer, S., Tapia, A., Pesheck, L., and Davenport, J. Mobility and the First Responder. *Communications of the ACM*. March. 62-65.

17. Saydjari, O.S. (2004). Cyber Defense: Art to Science. Communications of the ACM. March, 53-57.

18. Turner, B.M. (1976). The organizational and interorganizational development of disasters. *Administrative Science Quarterly*, 21, 378-397.

19. Weick, K.E.and Roberts, K. (1993). Collective mind in organizations: Heedful interrelating on flight decks. *Administrative Science Quarterly*, 38, 357-381.

20. Yourdon, E. (2002). *Byte Wars: The Impact of September 11 on Information Technology*, New Jersey: Prentice Hall.